УДК 621.3.06

И.В. ЛИСИЦКАЯ, А.А. НАСТЕНКО, К.Е. ЛИСИЦКИЙ

БОЛЬШИЕ ШИФРЫ – СЛУЧАЙНЫЕ ПОДСТАНОВКИ. СРАВНЕНИЕ ДИФФЕРЕНЦИАЛЬНЫХ И ЛИНЕЙНЫХ СВОЙСТВ ШИФРОВ, ПРЕДСТАВЛЕННЫХ НА УКРАИНСКИЙ КОНКУРС, И ИХ УМЕНЬШЕННЫХ МОДЕЛЕЙ

Дополнительно обосновывается справедливость гипотезы о том, что большие шифры асимптотически являются случайными подстановками. Выполняется сравнение дифференциальных и линейных свойств шифров, представленных на украинский конкурс, и их уменьшенных моделей. Рассматриваются линейные и дифференциальные показатели финалистов конкурса AES шифров Rijndael, Serpent, а также Threefish. Устанавливается, что по дифференциальным и линейным показателям украинские шифры Калина, Мухомор и Лабиринт превосходят признанного мирового лидера блочного симметричного шифрования.

Введение

Одним из актуальнейших направлений развития современной криптологии считается совершенствование методологии оценки показателей стойкости блочных симметричных шифров к атакам линейного и дифференциального криптоанализа. В этой работе мы продолжаем обоснование новой точки зрения (новой идеологии) в вопросах оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа [1], которая строится на установленном в ходе исследований факте, что все современные блочные шифры после нескольких начальных циклов шифрования приобретают свойства случайных подстановок соответствующей степени [2-5 и др.].

Основой развиваемого подхода является положение, в соответствии с которым большие шифры повторяют свойства своих уменьшенных моделей. В частности, в наших работах [6,7] было показано, что большие версии шифров при использовании их в режиме зашифрования укороченных (16-битных и 32-битных) блоков данных повторяют законы распределения вероятностей переходов XOR таблиц и таблиц смещений линейных аппроксимаций, свойственные соответствующим законам распределения вероятностей своих уменьшенных версий. Последние, в свою очередь, после нескольких начальных циклов зашифрования приходят к законам распределения вероятностей переходов XOR таблиц и смещений таблиц аппроксимаций случайных подстановок. Но выполненные эксперименты коснулись только шифров Rijndael, ГОСТ 28147-89 и FOX.

Продолжая развивать это направление, в настоящей работе мы представляем материалы по дополнительному обоснованию справедливости отмеченной выше гипотезы. Теперь сравниваются дифференциальные и линейные свойства шифров, представленных на украинский конкурс: Калина, Мухомор, Лабиринт и их уменьшенных моделей. Мы дополнили этот список ещё тремя шифрами: Rijndael, Serpent и Threefish.

1. Методика выполнения исследований

Здесь мы воспользовались методикой исследований, предложенной в работе [6]. Большой шифр применяется как малый для шифрования блоков данных уменьшенной длины (зашифрованные блоки данных тоже усекаются до необходимого размера), при этом сохраняются все преобразования и внутренние связи большого шифра. Самое же примечательное при таком подходе – это то, что появляется возможность применить весь наработанный аппарат изучения показателей случайности малых версий шифров для определения показателей случайности больших шифров.

Правомерность использования такого подхода оправдывается тем, что все украинские шифры построены на основе сбалансированных схем и байтовых 8x8 подстановок. Поэтому они не имеют особых дифференциальных характеристик, как в шифре DES, получающихся из-за наличия циклов с переходами обнуляющего типа [8].

В первом случае можно использовать 16-битные блоки открытых и соответствующих им зашифрованных текстов. Здесь мы приходим к условиям, в которых исследовались малые модели шифров [2-5 и др.]. Вычислительных ресурсов хватает для построения всей дифференциальной таблицы (большой шифр работает как его уменьшенная 16-битная версия).

Очевидно также, что при рассматриваемом подходе можно построить и уменьшенную таблицу смещений линейных аппроксимаций.

Во втором случае можно строить переходы для отдельной строки дифференциальной таблицы или смещения таблицы линейных аппроксимаций при использовании большого шифра для шифрования 32-битных блоков данных. Мы в этой работе воспользуемся 16-битными фрагментами входныъх и выходных блоков данных.

Дальнейший материал посвящен изложению результатов применения этой методики для исследования дифференциальных и линейных свойств украинских шифров, а также шифров Rijndael (AES), Serpent, Threefish и IDEA.

2. Сравнение дифференциальных и линейных показателей больших шифров и их уменьшенных моделей

*Дифференциальные свойства блочных симметричных шифров.*В первой серии экспериментов были рассмотрены дифференциальные свойства шифров, представленных на украинский конкурс, и их малых версий. В табл. 1 обобщены результаты таких экспериментов для шифров Мухомор, Калина, Лабиринт и ADE для 30 случайно взятых мастер-ключей. Описание малых версий этих шифров можно найти в работе [8].

Таблица 1

Поцикловые значения максимумов переходов XOR таблиц для полных версий украинских шифров

Число циклов	Калина	ADE	Лабиринт	Мухомор
1	19,47	65536	18	19,13
2	19,0	20	20	18,8
3	19,13	20	18	19,4
4	19,2	18	20	19,13
5	19.27	18	20	19,07
6	18,87	20	20	19,6
7	19,47	20	20	19,27
8	19.2	18	18	19,13
9	19,0	18	18	19,13
10	19,33	18	18	19,276

Заметим, что рассмотренные шифры по спецификациям имеют Мухомор-128 - 11 циклов зашифрования, Лабиринт - 8 циклов, Калина 128/256 - 14 циклов, ADE 128/128 - 10 циклов, Rijndael - от 10-ти до 14-ти циклов в зависимости от длины блока и ключа. В табл. все эксперименты приведены к 10-ти циклам зашифрования.

В табл.2 представлены результаты экспериментов с малыми версиями этих же шифров (для 30 ключей зашифрования).

Таблица 2

Поцикловые значения максимумов переходов таблиц полных дифференциалов для уменьшенных моделей украинских шифров

Число циклов	Мини-Калина	Мини-ADE	Мини-Лабиринт	Мини-Мухомор
1	3732,48	16384	37,5	65536
2	382,4	3353,6	**19,04**	5770,24
3	**19,36**	307,2	19,24	1802,24
4	19,14	20,54	19,04	125,53
5	19,2	**19,08**	19,14	29,7
6	19,36	19,24	19,24	**18,88**
7	18,93	18,87	19,33	18,67
8	19,27	19,27	18,67	19,00
9	18,93	19,20	19,00	18,00
10	18,87	18,73	18,00	18,67

Из представленных данных видно, что большие шифры, также как и малые их модели, действительно после нескольких (а то и сразу) начальных циклов зашифрования приходят к стационарным состояниям, повторяющим дифференциальные показатели случайных подстановок.

Примечательно, что малые модели шифров во всех случаях показывают динамику перехода к стационарному состоянию худшую, чем их большие прототипы. Наибольшее различие по динамике перехода (пять циклов) имеет шифр Мухомор. Это означает, что в его уменьшенной модели не удалось повторить все особенности оригинального преобразования. Мы уже отмечали в работе [9], что в этом шифре не удалось отмасштабировать SL-преобразование, и оно было заменено случайной подстановкой. Для шифра ADE разница для большой и уменьшенной модели составила четыре цикла, для Калины - три, для Лабиринта - два. Нужно также не забывать, что большие шифры имеют существенно увеличенный размер битового входа в шифры, поэтому они быстрее становятся случайными подстановками.

В табл. 3 представлены результаты оценки поцикловых значений максимумов таблиц линейных аппроксимаций украинских мини-шифров вместе со значениями среднеквадратических отклонений. И в этом случае эксперимент для каждого шифра проводился на 30 ключах зашифрования.

Таблица 3

Поцикловые значения максимумов смещений таблиц линейных аппроксимаций мини-шифров со значениями среднеквадратических отклонений (30 ключей)

Число циклов	Мини-Калина	Мини-Мухомор	Мини-Лабиринт	Mini-ADE
1	9671,1±867	32768±0	3178±777	16384
2	3370,6±301	12839,3±1031	980±193	9093,10±94,37
3	836,8±15	6400±697	825,4±14	3509,8±62,37
4	832,2±21	1797,6±347	825,6±23	828,56±7,58
5	838,6±21	837,8±47	817,2±11	820,52±5,48
6	835,5±33	815,6±24	824±21	819,92±5,81
7	821,5±22	817,2±20	823,4±30	818,55±5,35
8	827,3±18	815,8±15	833,6±35	837,34±5,91
9	813,3±21	815,5±15	824,8±24	814,95±6,21
10	834±28	810±17	819±17	822,54±7,13

Результаты вычислительного эксперимента по определению поцикловых средних значений максимумов линейных корпусов для больших версий украинских шифров представлены в табл. 4 в виде модульных значений максимальных смещений.

Таблица 4

Поцикловые значения максимумов смещений таблиц линейных аппроксимаций шифров со значениями среднеквадратических отклонений (30 ключей)

Число циклов	Калина 30 ключей	Мухомор 30 ключей	Лабиринт 1 ключ	ADE 5 ключей
1	11008,392± 1785,34	824,742± 20,1286	– 790	32768
2	817,271± 27,6348	818,621± 25,9742	839	3914.,4
3	817,718± 21,3851	827,431± 21,2352	-816	9523,2
4	814,19± 26,7792	824,193± 17,8115	832	1224,6
5	837,349± 28,2712	831,753± 25,7731	885	811,2
6	810,733± 29,3801	814,155± 28,9121	810	832,8
7	820,384± 20,752	820,975± 20,2673	– 834	827,4
8	837,917± 23,2539	823,024± 18,853	835	822,4
9	809,273± 22,186	810,196± 22,9352	– 809	826,8
10	821,755± 25,5737	821,316± 25,849	– 806	802,8

Как видно из представленных результатов, шифр Калина обладает средним значением максимума таблицы линейных аппроксимаций (820), практически не зависящим от используемых ключей шифрования (среднеквадратическое отклонение не превышает 30), харак-

терным для случайной подстановки степени 2^{16}. Это значение БСШ Калина достигает после 2-х циклов шифрования, что примечательно, так как предельных дифференциальных показателей случайной подстановки данный шифр достигает после 3-х циклов шифрования. Из этого факта можно сделать вывод, что эффективность цикловых преобразований в отношении защищенности от атак линейного криптоанализа у БСШ Калина немного выше, чем в отношении защищенности от атак дифференциального криптоанализа.

БСШ Мухомор достигает среднего значения максимума смещения линейного корпуса (820), характерного для случайной подстановки степени 2^{16}, уже после первого цикла шифрования, так же, как и среднего значения максимума дифференциального перехода (19), характерного для случайной подстановки аналогичной степени. Как видно, шифр Мухомор превосходит по эффективности цикловых преобразований в отношении защищенности от атак как дифференциального, так и линейного криптоанализа шифр Калина.

Близкие к Мухомору показатели показывает и шифр Лабиринт. Шифр ADE приходит к стационарному значению максимума смещения лишь на пятом цикле (здесь использована исходная версия шифра ADE [10] - без коррекции).

Следует заметить, что в табл. 4 представлены результаты для разного объёма ключевого материала. Дело в том, что базовый алгоритм подсчёта смещений таблиц линейных аппроксимаций вычислительно оказался более сложным по сравнению с алгоритмом построения дифференциальных таблиц. Удалось существенно продвинуться вперед в связи с найденным в Интернете описанием быстрого алгоритма расчёта линейных аппроксимационных таблиц (ЛАТ) [11].

В табл. 5 проведены результаты оценки временных затрат на расчет 1 строки ЛАТ, ЛАТ для всего набора циклов (максимальное число циклов 10), а также ЛАТ для всего набора циклов на 30-ти ключах.

Таблица 5

Временные затраты на построение линейной аппроксимационной таблицы

Алгоритм	$T_{1\ строки}$	$T_{1\ таблицы}$	$T_{10\ раундов}$	$T_{30\ ключей}$
Базовый	2,5 мин (2^{32} операций)	113 дней (2^{48}операций)	3 года ($\approx 2^{51}$операций)	92 года ($\approx 2^{56}$операций)
Ускоренный	$\approx$ 2 mc	2,5 мин (2^{32}операций)	25 мин ($\approx 2^{35}$операций)	12,5 ч ($\approx 2^{40}$операций)

Далее приведем результаты исследования дифференциальных и линейных свойств ещё для трех современных шифров: Rijndael, Serpent, Threefish. Были взяты полные версии этих шифров. Длина ключа и блока для Rijndael-я и Serpent-а одинакова и равна 128 битам, а в реализации шифра Threefish использовалась длина для блока и ключа 512 бит.

В табл. 6 представлены результаты распределения значений ячеек таблицы XOR-разностей для 16-битных сегментов шифртекстов всех трех шифров (Rijndael – 10 циклов шифрования, Serpent – 32 цикла, Threefish –72 цикла) и случайной подстановки степени 2^{16}.

Из табл. 6 следует, что распределения значений ячеек таблиц XOR-разностей для 16-битных сегментов шифртекстов для всех трех шифров после всех циклов преобразований очень близки к результатам, полученным вычислительным путём для случайной подстановки.

Результаты свидетельствуют также о том, что результирующие дифференциальные свойства шифров не связаны со свойствами S-блоков шифра, а являются общим свойством шифра, как случайной подстановки. Хорошим примером служат результаты анализа шифра Threefish, в котором не используются S-блоки.

Далее в табл. 7 представлены поцикловые значения максимумов полных дифференциалов для 16-битных сегментов. Для криптоалгоритмов Serpent и Threefish показаны первые 10 циклов, чего вполне достаточно для обозрения того, что шифры реализуют свой асимптотический показатель среднего значения максимума полных дифференциалов. Вычисления проводились с использованием 10 различных ключей для каждого шифра.

Таблица 6

Сравнение распределений значений ячеек таблицы XOR-разностей для 16-битных сегментов шифртекстов БСШ и случайной подстановки порядка 2^{16}

Значение перехода $2k$	Количество переходов (расчет для подстановки)	Количество переходов (Rijndael)	Количество переходов (Serpent)	Количество переходов (Threefish)
0	2605070418	2604948298	2604933270	2604928534
2	1302484861	1302476170	1302501597	1302508996
4	325626184	325620651	325614188	325612232
6	54271858	54268159	54265223,5	54265483,9
8	6784085	6783987,73	6782692,47	6782055,87
10	678418	678135,4	678425,133	678148,067
12	56535	56512,2	56524,067	56449,467
14	4038	4045,33	4027,133	4061,533
16	252	252,6	261,267	249,467
18	14	13,93	15,267	13,667
20	1	0	0	0

Таблица 7

Поцикловые значения максимумов полных дифференциалов для 16-битных сегментов

Число циклов, r	MAX (Rijndael)	MAX (Serpent)	MAX (Threefish)
1	65536±0	18,93	65536
2	3652,26±630,31	19,24	65536
3	19,07± 1,44	18,64	65536
4	19,07±1,00	18,33	42440,04
5	18,87±1,23	18,75	30704,23
6	19,13±0,99	19,21	9534,57
7	19,27± 1,09	18,98	37,75
8	19,13± 1,43	18,37	19,27
9	19,06± 1,23	19,24	18,78
10	19,33± 1,30	19,63	18,44

Приведенные результаты также говорят о том, что шифрующие преобразования асимптотически для различных ключей зашифрования ведут себя как случайная подстановка, т.е. и для них оказываются справедливыми расчетные соотношения, которые используются для случайной подстановки. Представленные для анализа шифры по-разному выходят на асимптотический показатель среднего значения максимума. Rijndael – после 4-го цикла, шифр Serpent выходит на данный показатель уже с 1-го цикла шифрующего преобразования за счет наличия в алгоритме начальной перестановки. Threefish выходит на асимптотический показатель среднего значения максимума только с 8-го цикла. На основе полученных результатов можно, тем не менее, предложить подход к сравнению эффективности решений по построению алгоритмов шифрования (при прочих равных условиях) в виде минимального числа циклов алгоритма, при котором реализуется асимптотический показатель среднего значения максимума полных дифференциалов.

Линейные свойства блочных симметричных шифров. Анализ линейных свойств был выполнен при помощи быстрого алгоритма построения таблиц линейных аппроксимаций [11]. Для всех трех шифров был выполнен подсчет максимумов линейных корпусов с использованием 10 различных случайно сгенерированных ключей.

Для алгоритмов Serpent и Threefish показаны первые 10 циклов, чего вполне достаточно для того, чтобы удостовериться, что шифры приходят к своим асимптотическим значениям максимумов полных дифференциалов (свойственным случайной подстановке степени 2^{16}).

В табл. 8 приведены математические ожидания максимальных значений смещений линейных корпусов для всех исследуемых шифров в зависимости от числа циклов шифрования r.

Таблица 8

Математические ожидания максимальных смещений линейных корпусов полных моделей шифров

Число циклов, r	MAX (Rijndael)	MAX (Serpent)	MAX (Threefish)
1	0	810,4	32768
2	9284,27± 657,45	825,0667	32680,93
3	818,47± 26,88	828,2667	31306,13
4	815,0± 28,20	825,9333	23730,93
5	818,5± 18,53	828,4667	19722,67
6	815,97± 20,18	824,8667	19722,67
7	832,1± 33,19	820,3333	7899,8
8	823,13± 23,57	817,5333	844,067
9	829,9± 33,57	820,4	822,13
10	827,4± 25,29	816,6	815,8

Представленные результаты свидетельствуют о том, что и по линейным показателям блочные симметричные шифры после определенного начального числа циклов приходят к показателям случайной подстановки: Rijndael – после 4-го цикла, шифр Serpent приходит к установившемуся значению максимума линейного корпуса, характерному для случайных подстановок, уже с 1-го цикла шифрующего преобразования. Threefish выходит на асимптотический показатель среднего значения максимума только с 8-го цикла.

Таким образом, дифференциальные и линейные свойства шифрующих преобразований исследуемых шифров (при заявленном числе циклов преобразования) являются одним из проявлений свойств случайных подстановок.

Выводы

Рассмотрены дифференциальные и линейные свойства шифров, представленных на украинский конкурс по выбору национального стандарта шифрования, и шифров из числа лидеров конкурса NESSIE.

Результатами приведенных исследований подтверждено одно из центральных положений развиваемого в работе [1] подхода, в соответствии с которым большие шифры повторяют свойства своих уменьшенных моделей. Конечно, здесь речь идёт о приближениях, но для нас важен сам факт прихода больших шифров к стационарному состоянию, свойственному случайной подстановке.

Главный результат наших исследований состоит в том, что получены дополнительные свидетельства того, что и большие шифры асимптотически становятся случайными подстановками. А это означает, что показатели стойкости блочных симметричных шифров могут быть получены расчётным путём из формул, определяющих значения максимумов XOR таблиц и смещений таблиц линейных аппроксимаций, полученных для случайных подстановок [12,13].

Список литературы: 1. *Лисицкая И.В.* Методология оценки стойкости блочных симметричных шифров // АСУ и приборы автоматики. 2011. № 143. С. 123-133. **2.** *Исследование* циклических и дифференциальных свойств уменьшенной модели шифра Лабиринт / В.И. Долгов, И.В. Лисицкая, А.В. Григорьев, А.В. Широков // Прикладная радиоэлектроника. 2009. Т.8, №3. С. 283-289. **3.** *Исследование* дифференциальных свойств мини-шифров Baby-ADE и Baby-AES / В.И. Долгов, А.А. Кузнецов, Р.В. Сергиенко, О.И. Олешко // Прикладная радиоэлектроника. 2009. Т.8, №.3. С. 252-257. **4.** *Долгов В.И.* Дифференциальные свойства блочных симметричных шифров, представленных на украинский конкурс / В.И. Долгов, А.А. Кузнецов, С.А. Исаев // Электронное моделирование. 2011. Т.33, № 6. С. 81-99. **5.** *Кузнецов А.А.* Линейные свойства блочных симметричных шифров, представленных на украинский конкурс / А.А. Кузнецов, И.В. Лисицкая, С.А. Исаев // Прикладная радиоэлектроника. 2011. Т.10, №2. С. 135-140. **6.** *Лисицкая И.В.* Большие шифры - случайные подстановки / И.В. Лисицкая, А.А. Настенко // Радиотехника. 2011. Вып. 166. С. 50-55. **7.** *Лисицкая И.В.* Дифференциальные свойства шифра FOX / И.В. Лисицкая, Д. С. Кайдалов // Прикладная радиоэлектроника. 2011. Т.10, №2. С. 122-126. **8.** *Долгов В.И.* О роли схем разворачивания ключей в атаках на итеративные шифры / В.И. Долгов, А.А. Настенко // Прикладная радиоэлектроника, 2012. № 30. С. 247-252. **9.** Криптографические свойства уменьшенной версии шифра IМухоморI. / И.В. Лисицкая, О.И. Олешко, С.Н. Руденко и др. // Спеціальні телекомунікаційні системи та захист інформації. Збірник наукових праць, Київ. 2010. Вип. 2(18). С. 33-42. **10.**

Кузнецов А.А. Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption). / А.А. Кузнецов, Р.В. Сергиенко, А.А. Наумко // Прикладная радиоэлектроника. Харьков: ХТУРЭ. 2007. Т. 6, №2. С. 241-249. **11.** *Krzysztof Chmiel.* On Differential and Linear Approximation of S-box Functions / Biometrics, Computer Security Systems and Artificial Intelligence Applications. / Edited by Khalid Saeed, Jerzy Pejas and Romuald Mosdorf // Poland, Springer. 2006. P. 111-120. **12.** *Олейников Р.В.* Дифференциальные свойства подстановок / Р.В. Олейников, О.И. Олешко, К.Е. Лисицкий, А.Д. Тевяшев // Прикладная радиоэлектроника. 2010. Т.9, № 3. С. 326-333. **13.** *Долгов В.И.* Свойства таблиц линейных аппроксимаций случайных подстановок / В.И. Долгов, И.В. Лисицкая, О.И. Олешко // Прикладная радиоэлектроника. Харьков: ХНУРЭ. 2010. Т. 9, № 3. С. 334-340.

Поступила в редколлегию 23.06.2012

Лисицкая Ирина Викторовна, д-р техн. наук, доцент кафедры безопасности информационных технологий ХНУРЭ. Научные интересы: криптография, методы криптоанализа. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел.: +38 (057) 702-14-25, E-mail: ai@kture.kharkov.ua.

Настенко Андрей Александрович, аспирант кафедры безопасности информационных технологий ХНУРЭ. Научных интересов: криптография, методы криптоанализа. Адрес: Украина, 61166, Харьков, пр. Ленина, 14.

Лисицкий Константин Евгеньевич, студент ХНУРЭ. Научные интересы: криптография, методы криптоанализа. Адрес: Украина, 61166, Харьков, пр. Ленина, 14.